## REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendment and the following remarks.

Claims 1-16 are pending in this application. The Examiner issued a non-final Office Action, rejecting claims 1-4, 6-14, and 16 under 35 U.S.C. § 102(b) as being anticipated by PCT Published Application No. WO01/37496 to Lakhdar et al. ("Lakhdar"). The Examiner also rejected claims 5 and 15 under 35 U.S.C. § 103(a) as being unpatentable over Lakhdar in view of U.S. Patent Publication No. 2004/0111519 to Fu et al. ("Fu").

Applicant has amended the pending independent claims, claims 1, 8, 10 and 16, as shown above. No claims have been cancelled, and no new claims have been added. For the reasons stated below, Applicant respectfully submits that all claims pending in this application are in condition for allowance.

### *Claim rejections under 35 USC § 102*

Applicant respectfully traverses the rejection of claims 1-4, 6-14 and 16 under § 102. As explained below, Applicant maintains that the present invention, as claimed in each of the independent claims, is neither anticipated nor suggested by the Lakhdar reference. That said, in order to expedite prosecution of the application, Applicant has amended the claims by explicitly reciting that the sender-specific policies indicate how or whether a mail message should be further transmitted.

At the outset, it is clear that the present invention is fundamentally different from the invention disclosed in Lakhdar. Specifically, whereas the present invention relates to messages

that have been digitally signed, and in particular deals with the issue that it is possible to forge the contents of the "From" field in an email message, Lakhdar relates to providing a system in which messages are not expected to be signed by the user: in fact the entire point of the Lakhdar patent is that the digital signature is added by the relay. (See Lakhdar at page 8, lines 16-18: "A key feature is that the relay 1 handles all cryptography and digital signature operations for the client 2. These operations are carried out transparently to the user and require no input from him or her.")

Claim 1

With respect to the limitations "receiving a mail message intended for further transmission … , [and] determining whether said mail message contains a digital signature" recited in claim 1, the disclosure on page 9, lines 25-30, of Lakhdar, cited by the Examiner as teaching determining if a signature is present actually specifically refers to a client-side API:

> A client side interface API function block 41 receives messages via the client plug-ins 12. The messages are passed to encryption functions 37 which perform encryption and digital signing according to the policies for the users and addressees retrieved from the database 30. As described above, if the addressee is being addressed for the first time there is digital signing by default, however the outgoing message can not be encrypted.

Applicant respectfully submits that this is NOT a disclosure of determining whether a signature is present, as recited in claim 1.

Claim 1 also requires "receiving a mail message intended for further transmission ..., [and] attempting to verify the digital signature in said mail message...". The Examiner cites Lakhdar as disclosing this element at page 10 lines 4-7:

> Messages are retrieved from the retriever 23 and are decrypted where applicable and the signature is authenticated by functions 38 using the database 30. The header (sender, subject, date) is passed to the client computer 2 for display (after decryption) if it is selected by the user."

However, the claimed invention is a method in which the "determining whether said mail message contains a digital signature" step and the "attempting to verify the digital signature in said mail message" step are performed on the same message, whereas the cited passage in Lakhdar relates to a first operation that is performed on the outgoing message and a second operation performed on an incoming message.

Thus, without even addressing the question as to whether Lakhdar actually discloses either of these steps, Lakhdar at page 9, lines 25-30 makes it clear that the first step relates to handling of an outgoing message, and at page 10, lines 4-7 that the second step relates to handling of an incoming message.[1] Therefore Lakhdar clearly does not disclose the invention as claimed in claim 1, which recites checking the digital signature in an outgoing message intended for further transmission.

---

[1] Lakhdar clearly states (page 9 lines 13-16) that the retriever 23 is for incoming mail messages: "Referring now to Fig. 3 the relay 1 is shown in more detail. It interfaces on the server side with (a) an SMTP delivery module 20 and an SMTP server 21 for sending messages, and (b) with an IMAP/POP3 mail server 22 and an IMAP/POP3 retriever 23 for receiving messages."

Claim 1 then defines what happens if the signature can be verified: "if the mail message does contain a verified digital signature, and if a user corresponding to the verified digital signature corresponds to the sender indicated in the mail message..." The Examiner's citation to Lakhdar page 10 lines 1-10 is not understood. The citation:

> However, once a reply is received from the addressee his or her certificate is stored in the database 30 and there will be encryption/decryption from then on. Messages are retrieved from the retriever 23 and are decrypted where applicable and the signature is authenticated by functions 38 using the database 30. The header (sender, subject, date) is passed to the client computer 2 for display (after decryption) if it is selected by the user.

This clearly relates to authentication of signatures in incoming messages, NOT to checking of signatures of senders of outgoing mail, as recited in claim 1.

Claim 1 also requires specific action when there is no verified digital signature: "if the mail message does not contain a digital signature, or does not contain a verified digital signature corresponding to the sender indicated in the mail message, applying a default mail policy to said message." The Examiner cites Lakhdar at page 9, lines 1-5 as disclosing this limitation:

> If Y responds, the relay 1 captures Y's certificate on the return path. From then on the relay 1 will automatically encrypt and sign all outgoing messages to Y, and also decrypt all incoming messages.

This citation is not understood – it clearly relates to automatic encryption and signing of outgoing messages (and decryption of incoming messages), not to determining whether a

message contains a verified digital signature and applying a default mail policy to the message. As explained in paragraphs [0037]-[0039] of the published application, if it is determined that the message does not contain a digital signature, the process applies a restrictive default policy in deciding whether the message is compliant and should be transmitted. In the present invention, there is no insertion of a signature, as disclosed in the Lakhdar passage relied upon by the Examiner. This is particularly clear in view of the following disclosure on page 8, lines 29-30 of Lakhdar:

> The message is routed to Y via the relay 1. This is not encrypted, but is signed automatically by the relay 1 on behalf of X.

Thus the passage in Lakhdar cited by the Examiner does not relate to applying a default mail policy, as recited in claim 1.

The Examiner's reliance on Lakhdar at page 9, lines 25-30 as also disclosing the default policy is also not understood:

> The messages are passed to encryption functions 37 which perform encryption and digital signing according to the policies for the users and addressees retrieved from the database 30. As described above, if the addressee is being addressed for the first time there is digital signing by default, however the outgoing message can not be encrypted.

This passage does not relate to the limitation regarding the application of a default policy for e-mails that do not contain a verified digital signature. In fact, apart from the coincidental appearance of the words "policies" and "default," this passage does not relate to any of the limitations recited in claim 1.

Claim 1 now explicitly recites that sender-specific policies determine how or whether the mail message should be further transmitted. Accordingly, claim 1 is clearly patentable over Lakhdar, because that limitation is not disclosed or suggested in Lakhdar.

Claims 8, 10 and 16

These claims all include the key limitations discussed above:

- receiving a mail message intended for further transmission and determining whether said mail message contains a digital signature
- attempting to verify the digital signature
- if the mail message does contain a verified digital signature, and if a user corresponding to the verified digital signature corresponds to the sender indicated in the mail message, applying the user-specific policy associated with the user

Accordingly, claims 8, 10 and 16 are patentable for the reasons provided above with respect to claim 1.

Claims 2-7, 9 and 11-15

Claims 2-7, 9 and 11-15 are patentable because they depend upon patentable independent claims, and also because they recite additional limitations further distinguishing those claims from the prior art of record.

***Conclusion***

In view of the foregoing all of the claims in this case are believed to be in condition for allowance. Should the Examiner have any questions or determine that any further action is desirable to place this application in even better condition for issue, the Examiner is encouraged to telephone applicants' undersigned representative at the number listed below.

PAUL, HASTINGS, JANOFSKY & WALKER LLP
875 – 15th Street, N.W.
Washington, D.C. 20005
Tel: 202-551-1700

Respectfully submitted,

Date: June 3, 2010

By: _____
Aslan Baghdadi
Registration No. 34,542

AB/hjm

Customer No. 36183